UNITED STATES TRANSPORTATION COMMAND **USTRANSCOM INSTRUCTION 33-35**
Scott Air Force Base, Illinois 62225-5357 **17 September 2001**

Communications and Information

UNITED STATES TRANSPORTATION COMMAND PRIVACY ACT PROGRAM

NOTICE: This instruction is available electronically on the USTRANSCOM WWW Business Homepage "Library."

OPR: TCJ6-RII (Cora Holt) Approved by: TCJ6 (Brig Gen Gilbert R. Hawk)
Supersedes: USTRANSCOMI 37-11, 5 Feb 96 Pages: 21
Distribution: Electronic Publishing

This instruction establishes policies, procedures, and responsibilities for implementation of the United States Transportation Command (USTRANSCOM) Privacy Act Program governing the collecting, safeguarding, maintaining, using, accessing, amending, and disseminating of personal information maintained by USTRANSCOM systems of records. This instruction is applicable to all personnel assigned to USTRANSCOM. The components will follow their Service instructions for information maintained by systems of records generated within their area of responsibility. This instruction implements Federal law, Department of Defense (DOD), and Air Force (AF) regulations listed in Attachment 1, and contains additional instructions and guidance affecting the USTRANSCOM Privacy Act Program. Use in conjunction with those publications. This instruction does not apply to Freedom of Information Act (FOIA) requests, information from systems of records controlled by the Office of Personnel Management (although maintained by a DOD component), or requests for personal information from the General Accounting Office. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. System of Records Notice F033 AF CIC C, Privacy Act Request File, applies. Maintain and dispose of records created as a result of processes prescribed by this instruction in accordance with applicable USTRANSCOM records management disposition schedule. A USTRANSCOM member can file a civil suit against their respective Service for failure to comply with the Privacy Act.

SUMMARY OF REVISIONS:

Overall, generally updates the text and references Air Force Instruction (AFI) 33-332 for procedures for requesting access to records, appeal procedures, computer matching programs, and specific exemptions. Defines responsibilities of the Privacy Act Systems of Records Managers, Privacy Act officer, and USTRANSCOM members; world wide web (WWW) location of DOD Systems of Records; and penalties for violating the Privacy Act. Converts the series of this instruction from 37 to 33, clarifies applicability, adds two categories of information normally not releasable, changes system notice procedures, adds a new paragraph regarding posting personal information on the web, and changes training requirements to comply with Secretary of Defense (A&M) Memo of 9 June 2000. *Note: Since this instruction has been revised in its entirety, asterisks will not be used to identify revised material.*

1. REFERENCES AND SUPPORTING INFORMATION. References, related publications, abbreviations, acronyms, and terms used in this instruction are listed in Attachment 1.

2. POLICY. The Privacy Act of 1974 and this instruction apply to information in USTRANSCOM Privacy Act systems of records.

2.1. An official system of records must be:

2.1.1. Authorized by law or Executive Order.

2.1.2. Controlled by USTRANSCOM policy.

2.1.3. Needed to carry out a USTRANSCOM mission or function.

2.2. USTRANSCOM does not:

2.2.1. Keep records on how a person exercises First Amendment rights. EXCEPTIONS are when USTRANSCOM has the permission of that individual or is authorized by federal statute, or the information pertains to an authorized law enforcement activity.

2.2.2. Penalize or harass an individual for exercising rights guaranteed under the Privacy Act and will give reasonable aid to individuals exercising their rights.

2.3. USTRANSCOM will:

2.3.1. Keep paper and electronic records containing personal information and retrieved by name or personal identifier only in approved systems of records published in the Federal Register.

2.3.2. Collect, maintain, and use information in such systems only to support programs authorized by law or Executive Order.

2.3.3. Safeguard records included in the systems and keep them the minimum time required.

2.3.4. Keep the records timely, accurate, complete, and relevant.

2.3.5. Amend and correct records on request.

2.3.6. Let individuals review and receive copies of their own records unless an exemption for the system exists or records were created in anticipation of a civil action or proceeding.

2.3.7. Provide a review of decisions that deny individuals access to or amendment of their records.

2.4. Personal Notes. The Privacy Act does not apply to personal notes on individuals for use as memory aids to supervise or perform other official functions that are not shared with others and there is no USTRANSCOM directive that requires maintenance.

3. RESPONSIBILITIES:

3.1. The Command, Control, Communications and Computer Systems Directorate (TCJ6), Resources, Plans, and Policy Division (TCJ6-R), Resources Information Branch (TCJ6-RI), Resources Information Communications and Records Management Team (TCJ6-RII) Chief will serve as the USTRANSCOM Privacy Act officer. The Privacy Act officer will manage the program, guide and train, review the program at regular intervals, submit reports, review all publications and forms for compliance with this instruction, review systems notices, investigate complaints, answer general Privacy Act questions and correspondence, and staff denial recommendations.

3.2. Systems of Records Managers are the officials who are responsible for managing a system of records, including policies and procedures to operate and safeguard it. Systems Managers will decide the need for and content of systems, manage and safeguard the system, train personnel on Privacy Act requirements, protect records from unauthorized disclosure, alteration, or destruction, prepare systems notices and reports, answer Privacy Act requests, keep records of disclosures using Air Force (AF) Form 771, Accounting of Disclosures, and evaluate the systems annually. See Attachment 2 for sample AF Form 771.

3.3. Service Element Commanders, Directors, Chiefs of Direct Reporting Elements (DREs), Functional Managers, and Supervisors within USTRANSCOM are responsible for ensuring Privacy Act data under their control comply with the following:

3.3.1. USTRANSCOM Force Protection (TCFP) may request information for law enforcement under 5 United States Code, Section 552a(b)(7). TCFP must indicate in writing the specific part of the record desired and identify the law enforcement activity requesting the record.

3.3.2. USTRANSCOM will record promises of confidentiality to exempt from disclosure any "confidential" information under subsection (k)(2), (k)(5), or (k)(7) of the Privacy Act.

3.3.3. USTRANSCOM will collect personal information directly from the subject of the record when possible. Third parties may be asked when information must be verified, opinions or evaluations are required, the subject cannot be contacted, or the subject requests the information be obtained from another person.

3.3.4. USTRANSCOM will give a Privacy Act Statement (PAS) orally or in writing to anyone from whom personal information is collected for a system of records, and whenever an

individual's Social Security Number (SSN) is requested. A PAS must include four items: (See Attachment 3 for sample PAS.)

3.3.4.1. Authority: The legal authority is the United States Code or Executive Order authorizing the program the system supports.

3.3.4.2. Purpose: The reason the information is collected.

3.3.4.3. Routine Uses: A list of where and why the information will be disclosed outside DOD.

3.3.4.4. Disclosure: Voluntary or Mandatory. (Use Mandatory only when disclosure is required by law and the individual will be penalized for not providing information.) Include any consequences of nondisclosure in nonthreatening language. (*NOTE: Do this regardless of how you collect or record the answers. You may display a sign in areas where people routinely furnish this kind of information. Give a copy of the PAS if asked; however, do not ask the person to sign the PAS.)*

4. SOCIAL SECURITY NUMBERS (SSNs). SSNs are personal and unique to each individual. Protect them as For Official Use Only (FOUO). Do not disclose them to anyone without an official need to know. Executive Order 9397, November 22, 1943, authorizes using the SSN as a personal identifier. This order is not adequate authority to collect a SSN to create a record. When law does not require disclosing the SSN or when the system of records was created after January 1, 1975, the SSN may be requested; however, the individual does not have to disclose it. If the individual refuses to respond, use alternative means of identifying records. Military Services use the SSN as a service or employment number to reference the individual's official records. When requesting a SSN as identification (ID) to retrieve an existing record, do not restate this information. When requesting a SSN to create a record, advise the individual the statute, regulation, or rule authorizing the request for the SSN, the uses that will be made of the SSN, and if individual is legally obligated to provide the SSN.

5. REQUESTING ACCESS TO PRIVACY ACT RECORDS. USTRANSCOM members or their designated representatives may request a copy of their records in a system of records. Requester need not state why they want access to their records. Basic procedures for requesting access to records are detailed in AFI 33-332, Chapter 4, to include fees charged and denial procedures. (*NOTE: DOD Systems of Records published in the Federal Register can be reviewed at http://www.defenselink.mil/privacy/notices.)*

6. DENIAL AUTHORITIES. The Commander in Chief (CINC) and his designee, the Deputy Commander in Chief (DCINC) are the USTRANSCOM Privacy Act denial authorities. Access denials are processed within 5 workdays from receipt of the request for access. The system manager for the information requested will prepare the recommendation for access denial package to include a copy of the request, the record requested, and applicable exemption.

Coordinate access denial recommendations through the Command Privacy Act officer (TCJ6-RII). The Privacy Act officer will review the proposed denial and coordinate through the Chief Counsel (TCJA) and Public Affairs (TCPA) for signature by the command denial authority. Notification of denials to requesters will include statutory authority, reason, and pertinent appeal rights. Before you deny a request for access to a record, ensure that:

6.1. The system has an approved exemption, and the exemption covers each document. (All parts of a system are not automatically exempt.)

6.2. Nonexempt parts are segregated.

6.3. If a physician believes that release could harm the person's mental or physical health, procedures for providing medical records include:

6.3.1. Asking the requester for a physician's name and address to which the records can be sent. (Include a letter explaining to the physician that giving the records directly to the individual could be harmful.)

6.3.2. Offering the services of a military physician other than the one who provided treatment, if naming the physician poses a hardship on the individual.

6.4. Third-party information is not deleted from a record when the subject requests access, except as noted in paragraph 6.5., unless the record is covered by an established exemption. Presume that all information in a file pertains to the subject of the file.

6.5. Third-party personal data (such as SSN and home address) is not releasable. This action is not a denial.

6.6. Records compiled in connection with a civil action or other proceeding including any action where judicial or administrative adjudicatory proceedings are expected are withheld. This exemption does not cover criminal actions. Do not release attorney work products prepared before, during, or after the action or proceeding.

7. AMENDING THE RECORD:

7.1. Individuals may ask to have their records amended to make them accurate, timely, relevant, or complete. Systems managers routinely correct a record if the requester can show that it is factually wrong. Anyone may request minor corrections orally. Requests for more serious modifications should be in writing. After verifying the identity of the requester, make the change, notify all known recipients of the record, and inform the individual. Acknowledge requests for amendment within 10 workdays of receipt. Give an expected completion date unless the change is completed within that time. Final decisions must take no longer than 30 workdays.

7.2. USTRANSCOM will not usually amend a record when the change is based on opinion, interpretation, or subjective official judgment. This action constitutes a denial, and requesters may appeal. If the system manager decides not to amend or partially amend the record, send a copy of the request, the record, and the recommended denial reasons to the command Privacy Act officer, who will review the proposed denial and coordinate through TCJA and TCPA for signature by the command denial authority, CINC or DCINC. If the denial authority approves the request, amend the record and notify all previous recipients that it has been changed. Denial notification to requesters will include the statutory authority, reason, and pertinent appeal rights.

7.3. Requester should pursue record corrections of subjective matters and opinions through proper channels to the Civilian Personnel Flight (CPF) using grievance procedures or the specific Service Board for Correction of Military Records. Record correction requests denied by CPF or Service Board for Correction of Military Records are not subject to further consideration under this instruction.

8. APPEAL PROCEDURES:

8.1. Individuals may request a denial review by writing to the Secretary of the Air Force through the initial denial authority within 60 calendar days after receiving a denial letter. The command Privacy Act officer will complete the appeal package to include the original appeal letter, the initial request, the initial denial, a copy of the record, any internal records or coordination actions relating to the denial, denial authority comments on the appellant's arguments, and legal reviews, if applicable. The command Privacy Act officer will forward the appeal package to CIO-BIM/P, 1155 Air Force Pentagon, Washington, D.C. 20330-1155 through TCJA and TCPA for signature by the command denial authority, CINC or DCINC. If the denial authority reverses an earlier denial and grants access or amendment, notify the requester immediately. See AFI 33-332 for further information on appeal procedures.

8.2. Do not keep copies of disputed records in the Privacy Act case file. Use the file solely for statistics and processing of requests. Do not use the case file(s) to make any kind of determination about an individual. Document reasons for untimely responses.

9. PRIVACY ACT NOTIFICATIONS:

9.1. USTRANSCOM will include a Privacy Act warning statement in each USTRANSCOM publication that requires collecting or keeping personal information in a system of records. Also, include the warning statement when publications direct collection of SSN from individuals. The warning statement will cite legal authority and the system of records number and title. You can use the following warning statement: "This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by (United States Code citation and or Executive Order number). System of Records Notice (number and title) applies."

9.2. USTRANSCOM will publish notices in the Federal Register of new, changed, and deleted systems to inform the public of the records kept by USTRANSCOM, and give them an opportunity to comment. The Privacy Act also requires submission of new or significantly changed systems to the Office of Management and Budget (OMB) and both houses of the Congress before publication in the Federal Register. This includes starting a new system, instituting significant changes to an existing system, sending out data collection forms or instructions, and issuing a request for proposal or invitation for bid to support a new system.

9.3. At least 120 days before implementing a new system of records, system manager must send a proposed system notice through the command Privacy Act officer to CIO-BIM/P. Send notices electronically to anne.rollins@af.pentagon.mil using Microsoft Word. Mark changes to existing notices using the "track changes" tool in Microsoft Word. Follow procedures in Attachment 4. On new systems of records, system manager must include a statement that a risk assessment was accomplished and is available should the OMB request it.

9.4. System managers will review their system notices annually and submit changes to CIO-BIM/P through the command Privacy Act officer.

10. PROTECTING AND DISPOSING OF RECORDS:

10.1. Systems managers will establish appropriate safeguards to ensure the security and confidentiality of records and protection against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. The system manager will be responsible for data retained in the system of records, ensuring information maintained is current, and security procedures are complied with.

10.2. Information will be protected according to its sensitivity level. Consider the personal sensitivity of the information and the risk of loss or alteration. Most information in systems of records are FOUO. Contact TCFP for protection methods of FOUO material. AF Visual Aid (VA) 33-276 is used on file folders (affix to the folder tab, next to the file folder label); floppy disks (affix to the floppy disk, not to the disk jacket); computer tapes (affix to the computer tape disk reel); hard disk drive (affix to disk drive housing); and CD-ROM (affix to jewel box) to protect Privacy Act material. AF Form 3227, Privacy Act Cover Sheet, is used for protecting Privacy Act material, such as, letters, file folders, listings, etc.; handcarrying material to and from offices; and working with Privacy Act material at workstations.

10.3. Balance additional protection against risk and cost. For example, a password may be enough protection for an automated system with a log-on protocol. Classified computer systems, or those with established audit and password systems, are obviously less vulnerable than unprotected files or word processors in offices that are periodically empty.

10.4. Records must be transferred in a manner that prevents unauthorized disclosure of information contained in a system of records. Use sealed opaque envelopes to transfer Privacy Act material by mail. Use sealed opaque envelopes or affix a label over the string closure of Optional Form 65-B (holey-joe) to transfer inter-base and inter-office Privacy Act material. Do not transmit a record from a system of records orally (by telephone or otherwise) to anyone unless the disclosure is authorized under the Privacy Act and until the recipient's identity and need to know are fully verified. Store paper record material or electronic media (floppy disks, CD-ROM, computer tapes, etc.) in a lockable container (filing cabinet, desk, etc.), or in a secured room at all times when not in use during working hours, and at all times during nonworking hours. Local Area Network (LAN) access of Privacy Act protected files will be password protected with a log-on protocol authorized by the respective system manager. Do not leave Privacy Act records unattended and exposed at any time unless the entire work area is fully secured from unauthorized persons. Annotate each page of document containing Privacy Act material with the statement, "Personal Data – Privacy Act of 1974 Applies." (This includes correspondence containing SSNs.) Mark all rosters/listings, which contain personal information (home address, home telephone number, or SSN) "FOUO" and add one of the following statements:

10.4.1. Official, used for alert, recall, emergency notification, etc.: "This (roster/listing) contains personal information and is to be used for official purposes only."

10.4.2. Unofficial, used for social, special events planning: "This (roster/listing) contains personal information and is to be used for social or quasi-social, special events planning purposes. Written consent has been secured from each individual listed."

10.5. Within USTRANSCOM, destroy Privacy Act material by tearing into small pieces, shredding, pulping, pulverizing, melting, burning, or chemical decomposition to render material unrecognizable or beyond reconstruction. The destroyed material may then be placed in trash containers. USTRANSCOM *will not use recycling* as a method of destroying Privacy Act material. Clear magnetic tapes or other magnetic medium by degaussing, overwriting, or erasing. It is the system manager's responsibility to ensure this process is accomplished.

11. PRIVACY ACT EXEMPTIONS. A system manager who believes that a system of records needs an exemption from some or all of the requirements of the Privacy Act should send a request to CIO-BIM/P through TCJ6-RII. The request should detail the reasons for the exemption, the section of the Act that allows the exemption, and specific subsections of the Privacy Act from which the system is to be exempted, with justification for each subsection. Only CIO-BIM/P can approve exempt systems of records from any part of the Privacy Act. Denial authorities can withhold records using these exemptions only if CIO-BIM/P previously approved and published an exemption for the system in the Federal Register. Exemption types include:

11.1. General exemptions free a system from most parts of the Privacy Act.

11.2. Specific exemptions free a system from only a few parts.

11.2.1. Certain systems of records used by activities whose principal function is criminal law enforcement (subsection [j][2]).

11.2.2. Classified information in any system of records (subsection[k][1]).

11.2.3. Law enforcement records (other than those covered by subsection [j][2]). The Air Force must allow an individual access to any record issued to deny rights, privileges or benefits to which they would otherwise be entitled by federal law or for which they would otherwise be eligible as a result of the maintenance of the information (unless doing so would reveal a confidential source) (subsection [k][2]).

11.2.4. Statistical records required by law. Data is for statistical use only and may not be used to decide individuals' rights, benefits, or entitlements (subsection [k][4]).

11.2.5. Data to determine suitability, eligibility, or qualifications for federal service or contracts, or access to classified information if access would reveal a confidential source (subsection [k][5]).

11.2.6. Qualification tests for appointment or promotion in the Federal service if access to this information would compromise the objectivity of the tests (subsection [k][6]).

11.2.7. Information which the Armed Forces uses to evaluate potential for promotion if access to this information would reveal a confidential source (subsection [k][7]).

(NOTE: See AFI 33-332, Attachment 3 for further information on specific exemptions.)

12. DISCLOSING RECORDS TO THIRD PARTIES:

12.1. Before releasing personal information to third parties, consider the consequences, check accuracy, and make sure that no law or directive bans disclosure. Personal information can be released to third parties when the subject agrees orally or in writing. USTRANSCOM members consent to releasing their home telephone number and address when they sign and check the "Consent" block on the Individual Personnel Data Report maintained by the Manpower and Personnel Directorate (TCJ1). Before including personal information such as home address, home phone number, and similar information on social rosters or directories, ask for written consent statements. Otherwise, do not include the information.

12.2. You must get written consent before releasing marital status, number and sex of dependents, race, gross salary of military personnel (see paragraph 12.3. for releasable pay information), civilian educational degrees and major areas of study (unless the request for information relates to the professional qualification for federal employment), school and year of graduation, home of record, home address and phone number, age and date of birth, present or future assignments for overseas or for routinely deployable or sensitive units, and office and unit address and duty phone for overseas or for routinely deployable or sensitive units. *(NOTE: These are not all inclusive.)*

12.3. Consent is not required to release name, rank, and grade; service specialty codes; pay (including base pay, special pay, and all allowances except Basic Allowance for Quarters [BAQ] and Variable Housing Allowance [VHA]); gross salary for civilians; past duty assignments; present and future approved and announced stateside assignments; position title, office, unit address, and duty phone number; date of rank; date entered on active duty (EAD); pay date; source of commission; professional military education; promotion sequence number; military awards and decorations; duty status of active, retired, or reserve; active duty official attendance at technical, scientific, or professional meetings; and biographies and photos of key personnel.

12.4. Information that can be obtained by authorized individuals for official purposes on a need to know basis from existing systems of records in USTRANSCOM include:

12.4.1. Miscellaneous personnel management actions (alert or recall rosters, wartime, mobility, emergency actions or assignments, shelter duties or assignments, etc.); off-duty employment information; and *on a voluntary-provided basis only*, an individual's involvement in off-duty activities for rendering performance/evaluation reports.

12.4.2. Dependent (spouse and children) information (name, age, sex, nationality, home address, home telephone number, etc., and special needs such as availability of special education or treatment facilities. *NOTE: Dependent information used for unofficial or quasi-official use will be on a voluntary-provided basis only*.

12.5. Information for social rosters (name, address, phone number, official title or position; invitations, acceptance, regrets, protocol) to include dependent information will be obtained *on a voluntary-provided basis only.*

12.6. Information for special events planning (biographical data including, but not limited to: name, duty, and home address) telephone numbers; name of spouse and family; description of position in business and community affiliations with military-oriented civic organizations; and photos will be *on a voluntary-provided basis only*.

12.7. When disclosing other information, consider if the subject would have a reasonable expectation of privacy in the information requested, and would disclosing the information benefit

the general public? USTRANSCOM considers information as meeting the public interest standard if it reveals anything regarding the operations or activities of the agency or performance of its statutory duties. Balance the public interest against the individual's probable loss of privacy. Do not consider the requester's purpose, circumstances, or proposed use.

12.8. USTRANSCOM may release information without consent to:

12.8.1. Respond to Freedom of Information Act (FOIA) requests when information is releasable.

12.8.2. Use within DOD by officials or employees with a need to know.

12.8.3. Agencies outside DOD for a routine use published in the Federal Register. The purpose of the disclosure must be compatible with the purpose in the routine use. When initially collecting the information from the subject, the Routine Uses block in the Privacy Act Statement must name the agencies and reason.

12.8.4. The Bureau of the Census to plan or carry out a census or survey under Title 13, United States Code, Section 8.

12.8.5. A recipient for statistical research or reporting. The recipient must give advanced written assurance that the information is for statistical purposes only. (*NOTE: No one may use any part of the record to decide an individuals' rights, benefits, or entitlements. You must release records in a format that makes it impossible to identify the real subjects.)*

12.8.6. The Archivist of the United States and the National Archives and Records Administration (NARA) to evaluate records for permanent retention.

12.8.7. A federal, state, or local agency (other than DOD) for civil or criminal law enforcement. The CINC or his designee, the DCINC, must send a written request to the system manager specifying the record or part needed and the law enforcement purpose. The system manager may also disclose a record to a law enforcement agency if the agency suspects a criminal violation. This disclosure is a routine use for all DOD systems of records and is published in the Federal Register.

12.8.8. An individual or agency that needs the information for compelling health or safety reasons. The affected individual need not be the record subject.

12.8.9. Congress, a congressional committee, or a subcommittee, for matters within their jurisdictions.

12.8.10. A congressional office acting for the record subject. A published, blanket routine use permits this disclosure. If the material for release is sensitive, obtain a release statement first.

12.8.11. The Comptroller General or an authorized representative of the General Accounting Office on business.

12.8.12. A court order of a court of competent jurisdiction, signed by a judge.

12.8.13. A consumer credit agency according to the Debt Collections Act when a published system notice lists this disclosure as a routine use.

12.8.14. A contractor operating a system of records under a USTRANSCOM contract. Records maintained by the contractor for the management of contractor employees are not subject to the Privacy Act.

12.9. Service personnel may disclose the medical records of minors to their parents or legal guardians. The laws of each state define the age of majority. Services must obey state laws protecting medical records of drug or alcohol abuse treatment, abortion, and birth control. Outside the United States (overseas), the age of majority is 18. Unless parents or guardians have a court order granting access or the minor's written consent, they will not have access to minor's medical records overseas when the minor sought or consented to treatment between the ages of 15 and 17 in a program where regulation or statute provides confidentiality of records and he or she asked for confidentiality.

12.10. Systems managers must keep an accurate record of all disclosures made from any system of records except disclosures to DOD personnel for official use or disclosures under the FOIA.

13. COMPUTER MATCHING PROGRAMS. See AFI 33-332 for information on computer matching programs.

14. PRIVACY AND THE WEB. *Do not* post personal information on publicly accessible DOD web sites unless clearly authorized by law. Additionally, *do not* post personal information on non-publicly accessible web sites unless it is mission essential and appropriate safeguards have been established.

15. TRAINING. The Privacy Act requires training for all persons involved in the design, development, operation and maintenance of any system of records. More specialized training is needed for personnel who may be expected to deal with the news media or the public, personnel specialists, finance officers, information managers, supervisors, and individuals working with medical and security records. The above personnel are required to have annual training in the principles and requirements of the Privacy Act. USTRANSCOM training aids include USTRANSCOM Pamphlet 37-13, The Privacy Act Program - A Manager's Overview, available

on the business web page at Library/Publications/USTRANSCOM/Index 2/P37-13, and the annual on-site FOIA and Privacy Act training at USTRANSCOM.

GILBERT R. HAWK, Brigadier General, USAF
Director, Command, Control, Communications
and Computer Systems

4 Attachments
1. Glossary of References and Supporting Information
2. Sample AF Form 771
3. Sample Privacy Act Statement (PAS)
4. Procedures for Preparing a PAS Notice

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 9397, 22 November 1943, Numbering System for Federal Accounts Relating to Individual Persons

32 Code of Federal Regulations 806b-13, Air Force Privacy Act Program

Title 5, United States Code, Section 552a, as amended, The Privacy Act of 1974

Title 10 United States Code, Section 164, Armed Forces, Organization and General Military Powers, Combatant commands

Title 10 United States Code, Section 3013, Armed Forces Organization, Department of the Army

Title 10 United States Code, Section 5013, Armed Forces Organization, Department of the Navy

Title 10 United States Code, Section 8013, Armed Forces Organization, Department of the Air Force

Title 13 United States Code, Section 8, Census, Administration, General Provisions

Department of Defense Directive 5400.11, Department of Defense Privacy Program

Department of Defense Regulation 5400.11, Department of Defense Privacy Program

Air Force Instruction 33-332, Air Force Privacy Act Program

USTRANSCOM Instruction 33-26, USTRANSCOM Freedom of Information Act Program

Abbreviations & Acronyms – Not used.

Terms

Access. Allowing individuals to review or receive copies of their records.

Agency. For the purposes of disclosing records subject to the Privacy Act among Department of Defense (DOD) Components, the DOD is considered a single agency. For all other purposes to include applications for access and amendment, denial of access or amendment, appeals from denials, and recordkeeping as regards release to non-DOD agencies; each DOD Component is considered an agency within the meaning of the Privacy Act.

Amendment. The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

Computer Matching. A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidential Source. A person or organization who has furnished information to the Federal Government under an express promise that the person's or the organization's identity will not be disclosed or under an implied promise of such confidentiality if this implied promise was made before 27 September 1975.

Confidentiality. An expressed and recorded promise to withhold the identity of a source or the information provided by a source. The Air Force promises confidentiality only when the information goes into a system with an approved exemption for protecting the identify of confidential sources.

Denial Authority. The individuals with authority to deny requests for access or amendment of records under the Privacy Act.

Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

Individual. A living citizen of the United States or an alien lawfully admitted to the United States for permanent residence. The legal guardian of an individual has the same rights as the individual and may act on his or her behalf. No rights are vested in the representative of a dead person under this instruction and the term "individual" does not embrace an individual acting in an interpersonal capacity (for example, sole proprietorship or partnership).

Individual Access. To make available information pertaining to the individual by the individual or his or her designated agent or legal guardian.

Maintain. Includes collecting, safeguarding, using, accessing, amending, and disseminating personal information.

Matching Agency. The agency that performs a computer match.

Member of the Public. Any individual or party acting in a private capacity to include Federal employees or military personnel.

Minor. Anyone under the age of majority according to local state law. If there is no applicable state law, a minor is anyone under age 18. Military members and married persons are not minors, no matter what their chronological age.

Official Use. Within the context of this instruction, this term is used when employees of a DOD component have a demonstrated need for the use of any records or the information contained therein in the performance of their authorized duties.

Personal Identifier. A name, number, or symbol which is unique to an individual, usually the person's name or Social Security Number (SSN).

Personal Information. Knowledge about an individual that is intimate or private to the individual, as distinguished from that related solely to the individual's official functions or public life.

Privacy Act Request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Privacy Act Statement (PAS). A statement furnished to an individual when the individual is requested to provide personal information, regardless of the medium used to collect the information, to go into a system of records. A PAS is also furnished to an individual when asking them for their SSN.

Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Risk Assessment. An analysis considering information sensitivity, vulnerabilities, and the cost to a computer facility or word processing activity in safeguarding personal information processed or stored in the facility or activity.

Routine Use. The disclosure of a record outside the DOD for a use that is compatible with the purpose for which the information was collected and maintained by the DOD. The routine use must be included in the published system notice for the system of records involved. For example: "To the Veterans Administration to verify the physical disability of applicants for the purpose of authorizing monthly retirement disability payments."

Source Agency. A federal, state, or local government agency that discloses records for the purpose of a computer match.

System Manager. The individual who initiates a system of records, operates such system, or is responsible for a segment of a decentralized part of that system and issues policies and procedures for operating and safeguarding of information in the system.

System Notice. The official public notice published in the Federal Register of the existence and content of the system of records.

System of Records. A group of records under the control of a DOD component from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual and published in the Federal Register.

ACCOUNTING OF DISCLOSURES *(Continue on Reverse)*		1. NAME OF RECORD SYSTEM AND TITLE TYPE		2. OFFICE SYMBOL	
DATE A	NAME AND ADDRESS OF REQUESTER B	NATURE AND PURPOSE OF DISCLOSURE C	NAME OF INDIVIDUAL D	CONSENT OF INDIVIDUAL *(Check)* E	
				YES	NO - NOT REQUIRED

SAMPLE

AF FORM 771, 19750801 *(EF-V3)*

PRIVACY ACT STATEMENT - JOINT PERSONNEL SYSTEM

AUTHORITY: Title 5 United States Code, Section 301; Title 10 United States Code, Sections 164, 3013, 5013, and 8013; Executive Order 9397.

PURPOSE: To provide USTRANSCOM Commander in Chief, Deputy Commander in Chief, element commanders, directorates, direct reporting elements, functional managers, and supervisors: (1) A ready source of information for day-to-day operations and administrative determinations pertaining to assigned personnel, (2) A protocol listing to include spouses' names for social/special events planning. Use of the SSN is necessary for establishing a record and identification control in the automated system.

ROUTINE USE: Information will not be released outside of the Department of Defense.

DISCLOSURE: Voluntary: (1) The furnishing of civilian/military member information is voluntary; but failure to provide it may result in your not receiving/could hamper/could delay personnel support. (2) The furnishing of dependent information is voluntary.

PROCEDURES FOR PREPARING A PRIVACY ACT SYSTEM NOTICE

The following elements comprise a system of records notice for publication in the Federal Register:

1. System identification (ID) number. CIO-BIM/P assigns the notice number; for example, F033 AF PC A, where "F" indicates "Air Force," the next number represents the records management disposition series, and the final letter group shows the system manager's command. The last character "A" indicates that this is the first notice for this series and system manager.

2. System name. Use a short, specific, plain-language title that identifies the system's general purpose, limited to 55 characters.

3. System location. Specify the address of the primary system and any decentralized elements, including automated data systems with a central computer facility and input or output terminals at separate locations. Use street address, 2-letter state abbreviations, and 9-digit ZIP codes. Spell out office names. Do not use office symbols.

4. Categories of individuals covered by the system. Use nontechnical, specific categories of individuals about whom USTRANSCOM keeps records. Do not use categories like "all USTRANSCOM personnel" unless they are actually true.

5. Categories of records in the system. Describe in clear, nontechnical terms the types of records maintained in the system. List only documents actually retained in the system of records. Do not show source documents that are used to collect data and then destroyed. Do not list form numbers.

6. Authority for maintenance of the system. Cite the specific law or Executive Order that authorizes the program the records support. Cite the DOD directive or instruction or other instruction that authorizes the system of records. Always include title with the citations. *NOTE: Executive Order 9397 authorizes using the SSN. Include this authority whenever the SSN is used to retrieve records.*

7. Purpose(s). Describe briefly and specifically what USTRANSCOM does with the information collected.

8. Routine uses of records maintained in the system, including categories of users, uses, and purposes of such uses. The blanket routine uses that appear at the beginning of each agency compilation in the Federal Register apply to all system notices unless the individual system notice specifically states that one or more of them do not apply to the system. Also, list each specific agency or activity outside DOD to whom the records may be released and the purpose for such release.

9. Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system.

9.1. Storage. Indicate the medium in which the records are maintained; i.e., file folders, card files, microfiche, computer, etc. Storage does not refer to the container or facility.

9.2. Retrievability. Specify how the records are retrieved; i.e., name and SSN, or personal characteristics (such as fingerprints or voiceprints).

9.3. Safeguards. List categories of agency personnel having immediate access and those responsible for safeguarding the records from unauthorized use. Identify system safeguards (safes, vaults, guards, etc.), but not in such detail as to compromise system security.

9.4. Retention and disposal. Disposal and accounting of records will be in accordance with applicable records management disposition schedule. When appropriate, also state length of time records are maintained by the agency, when they are transferred to a Federal Records Center, length of retention at the Records center, when they are transferred to the National Archives, or destroyed. State how records protected by the Privacy Act are destroyed: any method that prevents compromise, such as tearing, burning, or shredding, so long as the personal data is not recognizable and beyond reconstruction; degauss or overwrite magnetic tapes or other magnetic medium. Reference to an agency regulation without further detail is insufficient.

10. Systems manager(s) and address. List the title and duty address of the system manager. For decentralized systems, show the locations and the position or duty title of each category of officials responsible for any segment of the system.

11. Notification procedure. List the title and duty address of the official authorized to tell requesters if their records are in the system. Specify the information a requester must submit; i.e., full name, military status, SSN, date of birth, or proof of identity, etc.

12. Record access procedures. Explain how individuals may arrange to access their records. Include the titles or categories of officials who may assist; i.e., the system manager.

13. Contesting records procedures. CIO-BIM/P provides this standard caption.

14. Record source categories. Show categories of individuals or other information sources for the system. Do not list confidential sources protected by subsections (k)(2), (k)(5), or (k)(7) of the Privacy Act.

15. Exemptions claimed for the system. When a system has no approved exemption, write "none" under this heading. Specifically list any approved exemption including the subsection in the Privacy Act.